PROCESS AND ADAPTIVE AND PROGRESSIVE SYSTEM FOR THE SECURED DISTRIBUTION OF FIXED PICTURES CODED IN WAVELETS

[0001] The present invention relates to the area of the processing of digital pictures [images] coded in wavelets.

[0002] The present invention proposes furnishing a system that permits the visual scrambling of and the restoration in a progressive and adaptive manner of the original content of a fixed digital picture coded in wavelets.

[0003] The general problem is to furnish a process capable of transmitting in a secure manner digital data corresponding to high-quality pictures in any digital format stemming from a coding in wavelets either directly or pre-recorded to a viewing screen and/or for being recorded on the hard disk or any other backup device belonging to a box connecting the telecommunication network to a screen of the monitor or television screen type while preserving the visual quality but avoiding any fraudulent use such as the possibility of making pirate copies of the digitally coded picture. The classic encryption techniques consist in a general manner in combining (according to operations of the addition or subtraction type) the original data with values generated in a pseudo-random manner and from an initialization key. The simple possession of this key therefore permits the complete decryption of the encrypted data, which latter substantially contains the totality of the original information.

[0004] European patent application with the reference number EP 1011269A1 entitled "System for Processing an Information Signal" describes a method for encrypting an information signal that can be applied to the case of fixed pictures. The method consists in adding a pseudo-random noise to the non-compressed original signal in such a manner as to obtain a new signal. The signal encrypted in this manner is then compressed with the aid of adequate standard

algorithms and then transmitted. As for the key, it is transmitted in a secure manner to the destination of the future user of the encrypted signal. This known method can be applied to the case of the pictures coded in accordance with the JPEG norm.

[0005] This document of the prior art makes no reference to the case of pictures coded by wavelets. Moreover, the possession of the key totally conditions the decryption of the transmitted signal.

[0006] In the article "An Integrated Approach to Encrypting Scalable Video", Eskicioglu et al., Proceedings of the 2002 IEEE International Conference on Multimedia and Expo, Lausanne, Switzerland the authors describe a process for generating, managing and updating encryption keys used for protecting a multi-broadcasted binary stream coding a video sequence and presenting properties of scalability (multi-layer). The described protection system of the streams is a system in which each layer is encrypted with a different secret key, which key is known by a group of users and can change in a periodic manner over the course of time and as a function of the number of users. The proposed system is therefore based on classic selective encryption technologies with the aid of one or several keys: All the data is presented in the protected stream and only it conditions the access to the content and as a consequence this prior art does not resolve the problem of high security, the subject matter of the present invention.

[0007] In the article "Protecting VoD the Easier Way", Griwodz et al., Proceedings of the ACM Multimedia, September 1998, the authors describe a process for the distribution via broadband networks or temporary servers and a point-to-point secure connection of protected multimedia contents whose access is controlled and traced. The initial stream coding the original audiovisual content is deliberately corrupted by a predetermined modification of certain bytes in the stream and a signal permitting its reconstruction is only transmitted subsequently to the client

at the moment of the visualization of the content: A key is first sent to the client that permits him to recalculate the placing of the corrupted bytes in the stream. Then, a signal containing the original bytes is sent to him after encryption in order to reconstruct the initial stream. The reconstruction of the stream is therefore conditioned by a key and consequently the process described in this document of the prior art does not contribute the high level of security proposed in the present invention.

[0008] The present invention refers more particularly to a device capable of transmitting in a secure manner a set of fixed digital pictures with a high visual quality to a display device and/or for being recorded in the memory of the backup device of a box connecting the telecommunication network to the display device while preserving the visual quality yet avoiding the possibility that these pictures can be copied in an illicit manner.

[0009] The invention concerns a process for the secured distribution of fixed digital pictures in accordance with a nominal format originating in wavelet coding represented by a binary stream constituted by at least one packet (relative to the organization of the binary sequence) containing at least one block grouping simple elements (e.g., coefficients) coded digitally in accordance with a method specified in the stream concerned and used by all the decoders capable of restoring it or decoding it in order to be able to display it correctly. This process comprises:

* A preparatory stage consisting and modifying at least one of the simple elements,

* A stage for transmitting

- A main stream in conformity with the nominal format constituted by the blocks and packets modified in the course of the preparatory stage and

- By a path separate from the main stream of complementary digital information permitting the reconstitution of the original stream from the calculation on the addressed

equipment as a function of this main stream and of this complementary information. This complementary information is defined as a set constituted by data, e.g., coefficients describing the original digital stream or extracts of the original stream) and by functions (e.g., the substitution or interchanging [swapping, permutation function). A function is defined as containing at least one instruction putting data and operators in a relationship. This complementary information describes the operations to be carried out in order to restore the original stream starting from said modified stream.

[0010] In the present invention the notion of "stream" is defined as a structured binary sequence constituted by simple and ordered elements representing data in coded form and responding to a given audiovisual standard or norm.

[0011] The fact of having removed part of the original data of the original stream during the generation of the modified main stream does not permit the restitution of this original stream from only the data of this modified main stream. The modified main stream is then called a "secured stream". A "secured distribution" is a distribution of secured streams.

[0012] In the present invention the term "scrambling" denotes the modification of a digital binary stream in accordance with appropriate methods in such a manner that this stream remains in conformity with the standard with which it had been generated while rendering it decodable and displayable on a visual information screen coded by this stream but altered from the view-point of human visual perception.

[0013] In the present invention the term "descrambling" denotes the process of restitution by appropriate methods of the original stream, which video stream that is restituted after the descrambling is identical, that is, without loss, to the original video stream.

[0014] The notion of "granular scalability" is defined from the English expression "granular scalability". Scalability is defined as the property that characterizes an encoder capable of encoding or a decoder capable of decoding an ordered set of binary streams in such a manner as to produce or reconstitute a sequence called a multi-layer sequence. Granularity is defined as the quantity of information that can be transmitted by each layer of a stream resulting from an encoding by layers, which stream is then also qualified as (granular). The scalabilities that are qualitative, spatial and in resolution are then defined. A stream has a "qualitative scalability" if it is organized according to an ordered structure of successive sub-layers whose addition permits the improvement of the visual quality of the picture.

[0015] A stream has a "spatial scalability" if it is organized according to an ordered structure of blocks of data coding information that is locally spatial in the picture.

[0016] A stream has a "scalability in resolution" if it is organized according to an ordered structure of blocks of data coding information permitting the decoding of the picture at a fixed level of resolution.

[0017] Scalability in resolution is defined as the possibility of decoding the picture according to several layers of resolution starting from a single binary stream representing the picture encoded by wavelets.

[0018] A stream has a "spectral scalability" if it is organized according to an ordered structure of blocks of data coding information permitting the decoding of a multi-component picture according to a fixed component.

[0019] The present invention proposes the protection of the digital picture coded in wavelets integrally based on the structure of the "bitstream" (binary sequence), which protection consists in modifying the targeted parts of the bitstream (relative to the modeling by wavelets) and its

characteristics. Certain true values are extracted from the bitstream and are stored as complementary information and in their place random or calculated values or interchanged values are put in their places, which is done for the entire digital stream. Thus, the scrambler adds "decoys" for the decoder, that receives a binary stream at the input that is completely in conformity with the original digital format but from which the decoded and displayed picture is not acceptable from the viewpoint of human visual perception. The scrambling module makes an analysis of the bitstream and selects the locations of the bitstream where it introduces perturbations. A perturbation is defined as being a change (e.g., a change of value, sign inversion, saturation, thresholding) or a substitution by a random or calculated value or a permutation. The scrambling/descrambling process realized is without loss of quality for the original picture. The scrambling operation is advantageously also realized with a decoding/partial encoding of the bitstream representing the encoded picture.

[0020] The present invention advantageously permits the protection of a digital picture coded in a stream with a property of spatial scalability.

[0021] The present invention advantageously permits the protection of a digital picture coded in a stream with a property of scalability in resolution.

[0022] The present invention advantageously permits the protection of a digital picture coded in a stream with a property of scalability in quality.

[0023] The present invention advantageously permits the protection of a digital picture coded in a stream with a property of spectral scalability.

[0024] The scrambling operation is also advantageously realized with a complete previous decoding of the bitstream representing the encoded picture, then a re-encoding before modification in a stream with properties of scalability.

[0025] Inversely to the majority of encryption systems already known to an expert in the art, the principle described above permits the ensuring of a high level of protection while reducing the volume of information necessary for the decoding carried out in a progressive and adaptive manner.

[0026] The protection, realized in a manner in conformity with the invention, is based on the principle of the suppression and/or replacement of information coding the original visual signal by any method, whether: Substitution, modification, permutation or shifting of the information. This protection is also based on the knowledge of the structure of the stream at the output of the visual encoder: The scrambling is a function of the structure of said digital stream. The reconstitution of the original stream is carried out on the addressed equipment from the modified main stream already present or available (e.g., on a CD or DVD) or sent in real time to the addressed equipment and from the complementary information sent in real time at the moment of viewing comprising data and functions executed with the aid of digital routines (set of instructions).

[0027] Given knowledge of the manner with which the modeling, compression and encoding in wavelets of the picture are carried out by the wavelets coder and/or the given standard or norm, it is always possible to extract the main parameters from the bitstream that describe it and that are sent to the decoder.

[0028] Many scrambling systems have an immediate effect, that is to say, either the original stream is totally scrambled or the original stream is not scrambled at all, and likewise for the systems for descrambling the visual content. It is difficult with rigid systems of this type to satisfy the management of the rights of the users and the quality of service of multi-user, multi-application and multi-service client-server systems, that is to say, to adapt the services as a function of the different profiles of the users and of their rights.

[0029] "Profile" of the user denotes a digital file comprising descriptors and information specific to the user, e.g., his cultural preferences and his cultural and social characteristics, his habits of use such as the frequency of using viewing means, the average time of displaying scrambled and/or descrambled fixed pictures, the frequency of viewing a scrambled and/or descrambled sequence, or any other behavioral characteristic regarding the use of fixed pictures and successions of fixed pictures. This profile is formalized by a digital file or a digital table that can be used by computer means and is located in the server and/or the decoder box of the client.

[0030] "Hardware profile" of the user denotes a digital file comprising descriptors and information specific to the viewing hardware of the user, e.g., the resolution of his viewing screen, the calculating power of the fixed picture decoder or any other physical characteristic with respect to the use of fixed pictures or a succession of fixed pictures. This profile is formalized by a digital file or a digital table that can be used by computer means and is located in the server and/or the decoder box of the client.

[0031] The present invention has the problem of remedying the disadvantages of the prior art by proposing a system for the adaptive and progressive descrambling of the content viewed as a function of the profile and of the rights of the users.

[0032] In the present invention an adaptive and progressive descrambling of the content viewed is applied as a function of the profile and of the rights of each user. The server sends only the parts of this complementary information that has a structure characterized by a "granular scalability" for supplying the user with a content more or less scrambled as a function of certain criteria, profiles and rights. The digital streams encoded in wavelets have the properties of granular scalabilities that are spatial, qualitative and in resolution.

[0033] The granularity of this complementary information is relative to the degree of scrambling. For example, the fixed pictures are completely scrambled once for all the users. Then, the server sends all or part of this complementary information in such a manner that the picture or the succession of fixed pictures appears more or less scrambled to the user. The transmitted content of this complementary information and a content viewed on the viewing screen of the user are functions of each client and the server manages and carries out the sending in real time at the moment of the viewing by each user.

[0034] In its most general meaning the present invention relates to a process for the secured distribution of digital fixed pictures in the form of streams comprising sequences of data each containing a part of the information of the picture, which process comprises a stage for the modification of the original stream by modifying at least a part of these data sequences, which modification produces a stream modified in the same nominal format as the original stream, and which process comprises a stage for the transmission of the modified stream and a stage for reconstruction with the aid of a decoder in the addressed equipment, characterized in that the reconstruction is adaptive and progressive as a function of information coming from a digital profile of the addressed user.

[0035] This modification advantageously produces a modified main stream and complementary information permitting the reconstruction of the original stream by a decoder, which process comprises a stage for the transmission of the modified stream and also comprises a stage for the transmission to the addressed equipment of a subset of this modification complementary information, which subset is determined as a function of information coming from a digital profile of the addressee.

[0036] This modification advantageously produces a modified main stream and complementary information permitting the reconstruction of the original stream by a decoder, which process comprises a stage for the transmission of the modified stream and also comprises a stage for the transmission to the addressed equipment of a subset of this modification complementary information, which subset is determined as a function of information coming from a hardware profile of the addressee.

[0037] Furthermore, this original stream is coded in accordance with a process for coding in wavelets.

[0038] This original stream advantageously has a property of scalability in resolution.

[0039] This original stream advantageously has a property of spatial scalability.

[0040] This original stream advantageously has a property of qualitative scalability.

[0041] This original stream advantageously has a property of spectral scalability.

[0042] In a variant the modified main stream is available on the addressed equipment prior to the transmission of the complementary information to the addressed equipment.

[0043] According to a variant, part of the modified main stream is available on the addressed equipment prior to the transmission of the complementary information to the addressed equipment.

[0044] In another variant the modified main stream and the complementary information are transmitted together in real time.

[0045] The determination of said subset of this complementary information is advantageously based on the scalability properties of this original stream.

[0046] The determination of said subset of this complementary information is advantageously based on the properties of granular scalability of this complementary information.

[0047] Furthermore, the quantity of information contained in this subset corresponds to a level of scalability determined as a function of the profile of the addressee.

[0048] The type of information contained in this subset corresponds to a level of scalability determined as a function of the profile of the addressee.

[0049] This complementary information advantageously comprises at least one digital routine suitable for executing a function.

[0050] Said functions transmitted to each addressee are advantageously personalized for each addressee as a function of the session.

[0051] According to a variant said complementary information is encrypted in advance for each addressee as a function of the session.

[0052] According to a variant said complementary information is subdivided into at least two subparts.

[0053] According to an embodiment these subparts of the complementary information are distributed by different media.

[0054] According to another embodiment these subparts of the complementary information are distributed by the same medium.

[0055] In a variant all or part of the complementary information is transmitted on a physical vector.

[0056] In another variant the complementary information is transmitted on-line.

[0057] The type of information contained in this subset is advantageously updated as a function of the behavior of said addressee during the connection to the server or as a function of his habits or as a function of data communicated by a third party.

[0058] The quantity of information contained in this subset is advantageously updated as a function of the behavior of said addressee during the connection to the server or as a function of his habits or as a function of data communicated by a third party.

[0059] Furthermore, the process comprises a prior stage of analog/digital conversion in a structured format, which process is applied to an analog signal.

[0060] According to a variant a prior stage transcodes the digital stream from any format to a format with scalability properties.

[0061] Said fixed pictures advantageously constitute a succession of pictures fixed in time.

[0062] According to an embodiment said modification of said data sequences is different for at least two pictures of said succession of pictures.

[0063] According to another embodiment said modification of said data sequences of a picture of said succession of pictures includes the modification of said data sequences of the preceding pictures in the temporal order of the succession based on the properties of spatial and qualitative scalability of the transformations in wavelets.

[0064] The granular scalability of this complementary information constituted by said subsets is advantageously based on the qualitative, spatial and in-resolution scalabilities of the streams stemming from a transformation in wavelets of the pictures.

[0065] Moreover, the process is without loss of quality.

[0066] According to a particular variant the invention also concerns the processing of fixed pictures, e.g., pictures compressed in accordance with the JPEG2000 norm. In this instance it concerns a process for the secured distribution of fixed digital pictures, providing that during the reconstruction of said original stream an indelible and imperceptible trace is inserted in this original stream, which trace carries a non-ambiguous identifier.

[0067] According to a variant an indelible and imperceptible trace is inserted in the picture after reconstruction and decoding of said original stream, which trace carries a non-ambiguous identifier.

[0068] According to an exemplary embodiment this indelible and imperceptible trace can be detected by an adequate software that analyzes the reconstituted content.

[0069] This non-ambiguous identifier preferably authenticates the user.

[0070] According to a variant this non-ambiguous identifier authenticates the equipment on which the reconstruction algorithm of the original stream was executed.

[0071] According to another variant this non-ambiguous identifier identifies the session opened by the user during the course of which the reconstitution of the original stream is executed.

[0072] The scrambling session and the descrambling session are advantageously realized under the control of a secured server playing the part of trusted third party.

[0073] According to a particular embodiment this session is identified by a secured server with a register comprising for each session information about the session number, the identifier of the user or the identifier of the user equipment, the identifier of the content constituting the subject matter of the session and of a date-time group.

[0074] According to another embodiment a digital signature is calculated from the reconstituted stream, the inserted trace generates a unique and different signature for each reconstituted stream and this signature is stored on a secured server playing the part of trusted third party.

[0075] The stream reconstituted by the descrambling preferably has the same visual quality as the original stream and exists in a usable form only if it carries said trace.

[0076] The stream reconstituted by the descrambling advantageously exists in a usable form only if the digital signature extracted during an authenticity control stage is identical to the signature stored on the secured server playing the part of trusted third party.

[0077] The invention is advantageously applied to an audiovisual digital stream stemming from a proprietary norm or standard.

[0078] The invention also concerns a system for the secured distribution of fixed digital pictures comprising a server comprising means for broadcasting a modified stream, and a plurality of equipment provided with a descrambling circuit, which server also comprises means for recording the digital profile of each addressee and means for analyzing the profile of each of the addressees of a modified stream, which means controls the nature of the complementary information transmitted to each of these addressees.

[0079] Finally, the invention relates to a system for the secured distribution of fixed digital pictures in which the level (quality, quantity, type) of the complementary information is determined for each addressee as a function of the state of his profile at the moment of viewing the main stream.

[0080] The invention will be better understood with the aid of the following description, presented purely by way of explanation, of an embodiment of the invention with reference made to the attached figure.

[0081] The figure illustrates a particular embodiment of the client-server system in conformity with the invention.

[0082] The digital pictures are obtained with the aid of compression technologies based on wavelets (e.g., the fixed pictures in the JPEG-2000 norm, MPEG-4, JJ2000, JASPER, Kakadu, moving JPEG-2000). The concept of wavelets is an iterative scheme, that is to say, the repetition

of one and the same operation of filtering at weaker and weaker resolutions that generates streams characterized by a spatial, qualitative and in-resolution scalability. The original stream is reconstituted on the addressed equipment from the modified main stream and from the complementary information. The complementary information is divided into subsets and as a function of the user profile and one subset, several subsets or all of the complementary information is/are sent for partial or total descrambling of the pictures.

[0083] The complementary information sent to the user is advantageously encrypted prior to being sent with the aid of a key specific for each user.

[0084] The quantity of information contained in said subset is defined as the number of data and/or functions belonging to the complementary information sent to the addressee during the connection.

[0085] The type of information contained in said subset corresponds to a level of spatial, qualitative and in-resolution scalability determined as a function of the profile of the addressee. "Type" is defined as the nature of the data and/or functions belonging to the complementary information sent to the addressee during the connection to the server. For example, the type of data is relative to the habits of the addressee (complete subscription, partial subscription, payment by card, time of connection, duration of connection, regularity of the connection and of payments), of his environment (lives in a big city, the time at this moment), and to his characteristics (age, sex, religion, community).

[0086] The complementary information is advantageously constituted by a succession of subsets, each of which corresponds to a level of scalability defined in the original stream.

[0087] Said complementary information is composed by at least one function and the functions are personalized for each addressee relative to the connection session. A session is defined

from the time of connection, the duration, the type of the first stream viewed and the connected elements (addressees, servers).

[0088] This complementary information is subdivided into at least two subparts, each of which can be distributed by different media or by the same medium. For example, in the case of the distribution of the complementary information by several media a more complex management of the rights of the addressees can be ensured.

[0089] The transformation of the picture into wavelets (two-dimensional spatial signal) consists in applying a succession of high-pass and low-pass filters onto the original image that are worked up from the characteristics of the analysis wavelets. The operation of synthesis, that consists in reconstructing the picture from all or from a subset of the wavelets coefficients generated by the transformation follows a scheme of inverse filtering.

[0090] The application of a stage of wavelet transformation onto a digital image (that can be composed of one or several matrices with real or whole [entire] values) is equivalent to an operation of filtering on the lines and the columns of ... [word missing – "a matrix"?] or of matrices of values followed by a dyadic diminution (division by two) of the size. Thus, it generates 4 new matrices of wavelet coefficients at each stage that are called subbands and whose width and height are equal to one half the width and height of the transformed matrix (dyadic progression). Assume a picture I with width L, height H and resolution R. The application of a wavelet transformation state therefore generates 4 matrices of wavelet coefficients with the dimension (L/2, H/2): the subband LL_{R-1}, result of a horizontal (lines) and vertical (columns) low-pass filtering on the I picture, the subband LH_{R-1}, result of a horizontal low-pass and vertical high-pass filtering, the subband HL_{R-1}, result of a horizontal high-pass and vertical low-pass filtering, and the subband HH_{R-1}, result of a horizontal and vertical high-pass filtering.

[0091] Consider the transformation into wavelets at R levels (equivalent to R stages) of a picture. A wavelet transformation at R levels is associated with R+1 levels of resolution numbered from R to 0 with R and 0 corresponding respectively to the finest levels of resolution (initial picture) and the coarsest (approximate picture). Each subband stemming from the decomposition into wavelet of picture I is identified by its orientation (LL or HL or LH or HH) and its corresponding resolution level (comprised between 0 and R-1).

[0092] The original picture can be considered as the band LL_R. At each level I of the decomposition into wavelets (except the last i=0) the subband LL_i is thus decomposed into 4 new subbands LL_{i-i}, HL_{i-i}, LH_{i-i} and HH_{i-i}, and whose size is divided by two relative to LL_i. The process is iterated until subband LL_0 is obtained. Thus, for a wavelet transformation at R levels, 3R+1 subbands of wavelet coefficients are generated: LL_0, HL_0, LH_0, HH_0, HL_1, HH_1, ..., HL_{R-1}, LH_{R-1}, HH_{R-1}.

[0093] The reconstruction of the picture (synthesis) from the 3R+1 subbands of coefficients consists in applying an operation of inverse filtering to these wavelet coefficients followed by a dyadic augmentation of the size. A progressive reconstruction of the picture according to different resolution levels can thus be carried out. For example, by adding the 3 subbands of wavelet coefficients HL_{r-1}, LH_{r-1}, HH_{r-1} in the synthesis operation to the picture reconstructed from resolution r-1, a new picture with resolution r is obtained.

[0094] The single [unique] subband of wavelet coefficients LL_0 is an approximation of the original picture LL_R of which the resolution is 2^R times less than the original image.

[0095] As for the 3R subbands of wavelet coefficients HL_{r-1}, LH_{r-1}, HH_{r-1} ($\gamma \in [1,R]$) [The gamma might be an "r" in a different font.], they correspond to details in the picture, extracted at

resolution level r-1. The greater r is, the more the wavelet coefficients of the subbands are characteristic of finer and finer details (small) in the original image.

[0096] The wavelet coefficients stemming from the wavelet transformation of a picture are the spatially local characteristics of frequency information. The more r diminishes, the more the spatial zone characterized by a single wavelet coefficient increases (multiplication by a factor of 4 at each step).

[0097] A transformation into wavelets at R levels of a picture generates a "picture" called approximately lower resolution 2^R and 3R "pictures" called details at different resolutions (0 to R).

[0098] Consequently, a binary stream offering a granular scalability can be represented in the following form: $\{B_0, B_1, \ldots, B_{Ntot}\}$. Each B_1 represents a subset of bits and the binary stream can then be described as a sequence of subsets B_1 of binary symbols. Thus, a binary stream from a coding in wavelets has the property of "qualitative granular scalability" if and only if:

- The decoding of n ($n < Ntot$ where the binary stream is described as a sequence of Ntot subsets Bi) subsets of bits $B_0, B_1, \ldots, B_n$ implies a decoded picture I_d with quality Q_n, which quality is measured relative to the original picture I according to a predefined metric M calculated from subjective and/or objective elements, that is to say, $Q_n=M(I_d(n), I)$.

- When m ($m < n$) subsets B_1 are decoded, $\{B_0, B_1, \ldots, B_m\}$, then $Q_m < Q_n$.

- When p ($p > n$, $P < N$) subsets B_1 are decoded, $\{B_0, B_1, \ldots, B_m, \ldots, B_n, \ldots, B_p\}$, then $Q_n < Q_p$.

- When the Ntot subsets B_1 are decoded, Q_{Ntot} is maximum and $Q_{Ntot} \geq Q_1$ for $0 < I \leq Ntot$.

[0099] Likewise, a binary stream stemming from a coding in wavelets has the property of "scalability in resolution" if and only if:

- The decoding of n ($n < Ntot$) subsets of bits $\{B_0, B_1, \ldots, B_n\}$ implies a picture I_d with resolution R_n.

- When m ($m < n$) subsets B_1 are decoded, $\{B_0, B_1, \ldots, B_m\}$, then $R_m < R_n$.

- When p ($p > n$, $p < Ntot$) subsets B_1 are decoded, $\{B_0, B_1, \ldots, B_m, \ldots, B_n, \ldots, B_p\}$, then $R_n < R_p$.

- When the Ntot subsets B_1 are decoded, R_{Ntot} is maximum and $R_{Ntot} \geq R_i$ for $0 < I \leq Ntot$.

[0100] For example, a picture was scrambled by modifying (modification of the type addition/subtraction of noise, thresholding, permutation" a subset including N wavelet coefficients relative to one or several spectral components of the picture and/or belonging to one or several regions of interest in the original picture or to the entire picture and/or relative to different levels of resolution in the wavelet decomposition (from 0 to R-1) and/or belonging to one or several subbands (among LL, HL, LH and HH).

[0101] The adaptive and progressive descrambling of the picture consists in progressively descrambling the picture in several stages: First, n_0 ($0 < n_0 < Ntot$) wavelet coefficients modified by their original values are placed, then n_1 ($0 < n_1 < Ntot$) such as:

$$n_0 + n_1 + \ldots + n_p = Ntot.$$

[0102] The descrambling is adapted to the behavior of the client during the connection to the server as a function of the scrambling method used and the client profile.

[0103] An example of progressive descrambling will now be described. In this example the Ntot modified wavelet coefficients belong to subbands HL, LH and HH corresponding to 4

different levels of resolution (i.e., r, r+1, r+2, r+3). It consists in first replacing the n_0 wavelet coefficients belonging to subbands HL_r, LH_r and HH_r, then the n1 wavelet coefficients belonging to subbands HL_{r+1}, LH_{r+1} and HH_{r+1}, then the n_2 wavelet coefficients belonging to subbands HL_{r+2}, LH_{r+2} and HH_{r+2}, and finally the n_3 wavelet coefficients belonging to subbands HL_{r+3}, LH_{r+3} and HH_{r+3}. The first descrambling stage (replacement of the n_0 coefficients) attenuates in resolution and in extent the effects of the initial scrambling (suppression of the scrambling of the details of resolution r) but the details belonging to the upper levels of resolution (r+1, r+2 and r+3) are still degraded. The following stages attenuate the scrambling more and more in order to finally achieve a complete descrambling. This example is purely illustrative and should not be considered as limiting. The number of resolution levels affected by the initial scrambling can be comprised between 1 and R + 1. Therefore, as a function of this number the maximal number of descrambling stages can be comprised between 1 and R+1.

[0104] Another variant is to send ni coefficients belonging to subbands HL_{r+1}, LH_{r+1} and HH_{r+1} in several substages, thus increasing the number of progressive descrambling stages.

[0105] Another means of progressive descrambling consists in restoring the original wavelet coefficients relative to one of the C spectral components of the picture, then to two of the C components and so forth until the complete restoring of the original wavelet coefficients relative to the C components. One can then speak of progressive spectral descrambling. The number of descrambling stages also varies between 1 and C as a function of the number of components initially scrambled (between 1 and C).

[0106] According to an alternative embodiment the progressive descrambling of a scrambled picture consists in restoring the original wavelet coefficients belonging to a spatial zone predefined in the picture while maintaining a total scrambling of the rest of the picture. Assume

(L, H) the dimension of the original picture and (l, h) the dimension of the zone of interest to be descrambled on the original picture. It is supposed in this example that this zone is situated in the center of the picture but this zone can be defined anywhere in the original picture.

[0107] Assume r the level of resolution of the subband of wavelet coefficients to be restored. Then, the following formulas indicate the intervals [is, js] and [ie, je] of the indexes of the wavelet coefficients to be restored in the subbands of resolution r considered:

$$is = nlr / 2 - (1 / js = ncr / 2 - (h / 2^{r+1}), 2^{r+1}),$$

$$ie = nlr / 2 + (1 / 2^{r+1}), je = ncr / 2 + (h / 2^{r+1}),$$

where nlr, ncr are respectively the number of lines and of columns of the matrix of the wavelet coefficients in the subband considered. The progressive descrambling of the zone of interest is realized by successively restoring the original wavelet coefficients of each subband for each resolution: For example, LL_0, then HL_1, LH_1, HH_1, then HL_2, LH_2, HH_2 and so forth until HL_{r-1}, LH_{r-1} and HH_{r-1}.

[0108] According to another embodiment the progressive descrambling consists in first restoring the original wavelet coefficients belonging to subband LL, then the original wavelet coefficients belonging to all the LH subbands, then the original wavelet coefficients belonging to all the HL subbands and finally the original wavelet coefficients belonging to all the HH subbands. Thus, the scrambling of the details is progressively attenuated according to their orientations. The order of the types of subbands for which the wavelet coefficients are restored can advantageously be modified.

[0109] The invention will be better understood from a reading of an exemplary embodiment concerning a stream with the JPEG-2000 format. In this example the invention consists in

modifying the value of certain fields, especially the information necessary for a decoder for the reconstitution of the original stream.

[0110] The figure in the attached drawing represents a particular preferred embodiment of the client-server system in conformity with the invention.

[0111] The original stream 11 can be directly in digital form 111 or in analog form 101. In the latter instance analog stream 11 is converted by a coder (not shown) into a digital stream 111. In the remainder of the text "1" denotes the digital input stream corresponding to the fixed picture. The JPEG-2000 stream to be secured 1 is sent to an analysis and scrambling system 121 that generates a modified main stream 122 in the same JPEG-2000 format, a format identical to input stream 1 except that the values of certain elements of the stream have been replaced by values different from the original ones, and is placed in an output buffer memory. Complementary information 123 in any format and organized in layers of granular scalability contains information relative to the elements of the pictures that have been modified, replaced, substituted or shifted, as well as their value or emplacement in the original stream and has several subsets relative to its property of granular scalability.

[0112] The stream in JPEG-2000 format 122 is transmitted via telecommunication network 4 of the microwave, cable, satellite, etc. type to terminal 8 of the user and more precisely into its memory or onto its hard disk 85. When the user wishes to display fixed pictures present in his terminal, terminal 8 makes the request to display the fixed pictures present in its memory or on its hard disk 85. Server 12 verifies the rights of this user for this request. In order to achieve this, the server can use the data of this user contained in a database connected to server 12 and/or use a system based on a smartcard 82 connected to synthesis system 87. Two possibilities are then possible.

[0113] If the user does not have all the rights necessary for viewing the image, in which case JPEG-2000 stream 122 generated by scrambling system 121 present in the memory or on hard disk 85 is sent to synthesis system 87 via reading buffer memory 83. Synthesis system 87 does not modify it and transmits it identically to classic JPEG-2000 reader 81 and its content, degraded visually by scrambling system 121, is displayed on viewing screen 6. The user of terminal 8 thus sees a scrambled picture.

[0114] Alternatively, the user has the rights to view the picture. In this case the synthesis system addresses a viewing request to server 12 containing the information 123 necessary for the recovery of the original picture 101. Server 12 then sends, via telecommunication networks of the analog or digital telephone line, DSL (digital subscriber line) or BLR (local radio loop) type, via DAB (digital audio broadcasting networks or via digital mobile telecommunication networks (GSM, GPRS, UMTS) 5, at least one subset of complementary information 123 permitting the reconstitution of the picture in terminal 8, which stores this subset in buffer memory 86. Synthesis system 87 then proceeds to the restoration, in the scrambled JPEG-2000 stream that it reads in reading buffer memory 83, of the modified fields for which it knows the positions as well as the original values by virtue of the content of the complementary information read in buffer memory 86 for the descrambling of the picture. The quantity of information contained in complementary information 123 and sent to the descrambling system is specific, adaptive and progressive for each user and is a function of his rights, e.g., single or multiple use, right to make one or more private copies, delay in payment or payment in advance. In order to determine the quantity of information of complementary information 123 to send to terminal 8, server 12 consults the rights of the user in advance.

[0115] According to an embodiment a progressive descrambling of a picture for which the Ntot modified wavelet coefficients belong to subbands HL, LH AND HH corresponding to 4 different levels of resolution (that is to say, r, r+1, r+2, r+3) consists in first replacing the n_0 wavelet coefficients belonging to subbands HL_r, LH_r and HH_r, then the n_1 wavelet coefficients belonging to subbands HL_{r+1}, LH_{r+1} and HH_{r+1}, then the n_2 wavelet coefficients belonging to subbands HL_{r+2}, LH_{r+2} and HH_{r+2}, and finally the n_3 wavelet coefficients belonging to subbands HL_{r+3}, LH_{r+3} and HH_{r+3}. The first descrambling stage (replacement of the n_0 coefficients) attenuates in resolution and in extent the effects of the initial scrambling (suppression of the scrambling of the details of resolution r) but the details belonging to the upper levels of resolution (r+1, r+2 and r+3) are still degraded. The following stages attenuate the scrambling more and more in order to finally achieve a complete descrambling. The number of resolution levels affected by the initial scrambling is comprised between 1 and R+1 as a function of the number of resolution levels R selected for scrambling the stream. Therefore, the number of descrambling stages is comprised between 1 and R+1 as a function of this number. In this embodiment the sending of a subset of the complementary information containing the n_0 coefficients is carried out when the user connects, selects and downloads the picture that he desires. The picture selected is then displayed on his partially descrambled screen because it is calculated from the n_0 coefficients transmitted to the user terminal. If the user decides to see the picture in accordance with a higher resolution, the server proposes to the user that he pay a predetermined sum. If the user pays immediately by a classic remote payment means (credit card, ...), the server sends a second subset of the complementary information containing the n_1 coefficients. During the payment transaction the subsets of the complementary information concerning the following descrambling stages are sent and attenuate the scrambling more and more in order to finally

achieve a complete descrambling and the displayed picture is identical to the original picture. If the client does not accept to pay immediately, the coefficients will be sent progressively as a function of the arrival of the payment. In each transaction the server records the behaviors of the user and re-updates his profile in a database as a function of these behaviors.

[0116] The sent content of this complementary information 123 and the content visualized on the viewing screen of the client are functions of each client and the server manages and carries out the sending of these subsets in real time at the moment of viewing for each user, e.g., as a function of the price that the client is ready to pay.

[0117] Assume that fixed pictures are stored on the server with 10 different resolutions from R=1 to R=10, R=10 being the maximum resolution. If a client has a habit of ordering pictures with an average resolution, his subscription corresponds to the descrambling obtained with R = 5. If he wishes to obtain a high-resolution, e.g., a descrambling for R = 7, he must change his payment or subscription type. He can then obtain, if he so desires and by means, e.g., of a new payment the resolution R = 8, then R = 9 and finally R = 10. All these operations are managed by server 12 as a function of the behavior of each user and by using a database connected to server 12.

[0118] Likewise, another client who needs high-resolution pictures will take the subscription corresponding to the maximum resolution for R = 10. If this client has a delay in payment, the server will automatically send him pictures descrambled for R = 6, e.g., in order to remind him to put his payment in order.

[0119] As has been described, the level (quality, quantity, type) of complementary information is determined as a function of each addressee, as a function of the state of his profile at the moment of the transmission of the main stream and at least part of said profile is stored on

addressee equipment. For example, in the attached drawing part of the user profile is recorded on smartcard 82 connected to synthesis system 87 such as, e.g., the digital data concerning the frequency of connections or the regularity of payments. This same data and/or the rest of the profile can be located on server 12. The remainder of the profile can contain, e.g., the type of pictures that the user prefers.

[0120] In a variant the profile of the addressed is updated. The updating also depends on the time of the connection to the server (data relative to the behavior), namely, whether the client connects regularly (referring to his habits). Likewise, the profile of the addressee can be updated as a function of data recovered in a consumer database already existing on a server and relative to this client.

[0121] According to another exemplary embodiment the server transmits all or part of the complementary information to the user during several seconds of displaying the picture, then transmits fewer and fewer subsets of the complementary information in the course of time. Thus, the descrambling of the picture is less and less complete, thus giving the effect to the user that the picture displayed on his screen is becoming less and less comprehensible, therefore more and more scrambled. This functionality incites the user to purchase the rights to see the completely descrambled picture, given that he has partially seen the content.

[0122] According to another embodiment all or part of complementary information 123 is transmitted to the user on a physical vector such as a memory card or a smartcard 82.

[0123] According to another embodiment only part of the modified main stream is available on the equipment of the addressee: If the characteristics of viewing screen 6 only permit the displaying of a restricted number of resolutions (R = 1 to R = 5), the user only needs to recover part of the modified main stream 122. A part of the complementary information permitting him to

view the picture only in resolutions R = 1 to R = 5 will be sent by server 12 to user terminal 8 as a function of the profile and the rights of the user.

[0124] The example described below represents another preferred embodiment of the progressive and adaptive descrambling for digital pictures of stemming from the JPEG-2000 norm.

[0125] Analysis and scrambling module 121 generates complementary information 123 and sends it to the equipment of the addressee via network 5. Network 5 advantageously comprises a secure server on which complementary information 123 is stored. Module 121 also generates modified main stream 122 in the JPEG-2000 format, that is transmitted to hard disk 85 of the addressed equipment of the client by network 4. Network 4 advantageously comprises a multimedia server on which modified main stream 122 is stored. Scrambling module 121 also inserts into the meta-data of the modified main stream the identifier of the complementary information corresponding to this modified main stream and the physical address of secure server 5 on which this complementary information is stored.

[0126] The complementary information is characterized by the presence of said subsets corresponding to several layers of scalability, e.g. to the number of four. The first subset contains all the complementary information relative to the high quality of the original picture. The second subset contains a part of the complementary information relative to an acceptable quality. The third subset contains a part of the complementary information relative to a low quality while the image remains still visible but unusable. The fourth subset contains just the part of the complementary information corresponding to a minimum quality and the picture is poorly visible.

[0127] During the reconstitution of the original stream descrambling module 87 inserts an indelible trace imperceptible to the human eye into the reconstituted stream which trace carries a non-ambiguous identifier. The trace inserted into the stream can be detected by an adequate soft-

ware that has the ability to analyze the reconstituted content. The insertion of this trace and the descrambling are carried out in a sequential and progressive manner in such a manner that a stream that was scrambled by analysis and scrambling system 121 and then descrambled by module 8 exists in a form that can be used only if it comprises this non-ambiguous trace. During the descrambling and the sequential insertion of the trace the reconstitution is performed in such a manner that the trace is inserted progressively during the progressive descrambling. At the end of the descrambling the protection is ensured by the trace, that is substituted for the protection obtained by the scrambling.

[0128] An indelible trace imperceptible to the human eye is advantageously inserted into the picture after the decoding of the reconstituted stream.

[0129] A protected stream with scrambling module 12 and descrambled with this variant of descrambling module 87 is advantageously always a carrier of a protection: whether invisible, stemming from the insertion of the identifying trace, or whether visible, stemming from the adaptive and progressive descrambling.

[0130] This non-ambiguous identifier carried by the trace is advantageously relative to the identification of the interactive session opened by the user. The role of this non-ambiguous identifier is the authentication of the user, of the addressed equipment on which the picture is reconstructed and/or of the session opened by the user.

[0131] According to an embodiment during the descrambling stage the stream is reconstituted and an indelible and imperceptible trace is inserted. A digital signature of the reconstituted stream is then calculated, which signature is unique and different for each stream reconstituted by the insertion of the trace and the signature is stored on a secure server playing the part of a trusted third party.

[0132] The reconstituted stream advantageously exists in usable form only if the signature extracted during an authenticity check stage is identical to the signature stored on the secure server during the reconstitution.

[0133] The session is characterized by a number assigned by secure server 5 that plays the part of trusted third party between the user and the adaptation of the parameters characterizing the descrambling type. Secure server 5 assigns a specific number to each session that is backed up in a register. The information comprised in the register is the session number constructed from the identifier of the user or the identifier of his equipment 8, the identifier of the content of the picture constituting the subject matter of the session and of a date-time group in the ISO standard.

[0134] The identification of the content of the picture is made by descrambling module 87 that restores from the meta-data of the modified main stream the identity of the complementary information relative to the modified main stream and the physical address of network 5 where the secure server is located on which this complementary information is stored.

[0135] The reconstitution of the original picture is carried out in several stages. During the establishing of the session descrambling module 87 reads the identifier of the complementary information and the URL of secure server 5 in the meta-data of the modified main stream. Server 5 first sends said fourth subset of the complementary information that produces a picture of minimal quality, which picture can not be used and is poorly visible. This stage serves to confirm the identity of secure server 5. The second stage consists in sending to the descrambling module said third subset of the complementary information that renders the picture visible but still non-usable. This stage is necessary so that the client can decide whether he wishes to obtain rights for using the picture by viewing an outline of its contents. The client is sent said second

subset (corresponding to an acceptable quality) or said first subset (corresponding to a maximum quality) of the complementary information by means of the payment corresponding to the required quality as a function of his desire to obtain an acceptable or a maximum quality of the picture. A non-ambiguous trace is always present in the reconstituted stream independently of the subset used for the descrambling. This trace is intended to protect the intellectual property in conformity with the WIPO treaty (World Organization of Intellectual Property) of December 1996 stipulating that the data intended for the protection of intellectual property can be digital data.

[0136] The embodiments described above have the value of examples and do not constitute a limitation of the present invention.